Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A computer-implemented method of single sign-on user access to multiple web servers, comprising:

authenticating a user by a first web server, the first web server also providing a first type of service session functionality for the user in addition to an authentication functionality;

detecting a client request for a second type of service session functionality for the user at said first web server that is not provided by the first web server, said first web server determining a second web server providing the second type of session functionality for the user and in response thereto creating an encrypted authentication token related to the user and redirecting a web browser of the user to the second web server;

transmitting the encrypted authentication token from the first web server to the second web server via the user's web browser, wherein the authentication token comprises an expiration time and is digitally signed by the first web server;

authenticating the authentication token by the second web server; and

providing the second type of service session functionality for the user by the second web server.

2. (original) The method of claim 1 wherein the first web server and the second web server share a sub-domain.

3. (original) The method of claim 2 further comprising examining the expiration time of the authentication token at the second web server and allowing the user to conduct a session at the second web server only if the expiration time has not passed.

4. (original) The method of claim 3 wherein the authentication token comprises a cookie.

5. (original) The method of claim 4 wherein transmitting the encrypted authentication token from the first web server to the second web server comprises transmitting the encrypted authentication token from the first web server to the user, and then from the user to the second web server.

6. (original) The method of claim 5 wherein authenticating the user at the first web server comprises receiving a user name and password.

7. (original) The method of claim 6 wherein transmitting the encrypted authentication token from the first web server to a second web server comprises transmitting the authentication token from the first web server to a computer of the user; and transmitting the authentication token from the computer of the user to the second web server.

8. (original) The method of claim 7 wherein the first web server and the second web server comprise a federation of web servers.

9. (original) The method of claim 8 wherein authenticating the authentication token at the second web server comprises examining the cookie.

10. (original) The method of claim 9 further comprising URL encoding the authentication token.

11. (original) The method of claim 10 further comprising URL decoding the authentication token at the second web server.

12. (original) The method of claim 11 further comprising providing a web page to the user having a service selector.

13. (original) The method of claim 12 wherein the service selector comprises a hyperlink.

14. (original) The method of claim 13 wherein the hyperlink comprises a URL for the second web server.

15. (previously presented) The method of claim 7, further comprising:

sending the digitally signed authentication token to the web browser of the computing device by the first web server; and

sending the authentication token to the second web server by the web browser.

16. (original) The method of claim 15 further comprising allowing the user to conduct a session with the first web server.

17. (original) The method of claim 16 wherein the second web server shares a sub-domain with the first web server.

18. (previously presented) The method of claim 17 further comprising digitally signing the authentication token using public key encryption.

19. (original) The method of claim 18 further comprising confirming a match with the digital signature.

20-24. (canceled)

25. (previously presented) A system for single sign-on user access to multiple web servers, comprising:

a means for authenticating a user by a first web server, the first web server also providing a first type of service session functionality for the user in addition to an authentication functionality;

means for detecting a client request for a second type of service session functionality for the user at said first web server that is not provided by the first web server, for determining a second web server providing the second type of session functionality for the user and in response thereto creating an encrypted authentication token related to the user and for redirecting a web browser of the user to the second web server by said first web server;

a means for transmitting the encrypted authentication token from the first web server to the second web server via the user's web browser, wherein the authentication token comprises an expiration time and is digitally signed by the first web server;

a means for authenticating the authentication token by the second web server; and

a means for providing the second type of service session functionality for the user by the second web server.

26. (original) The system of claim 25 wherein the first web server and the second web server share a sub-domain.

27. (original) The system of claim 26 further comprising a means for examining the expiration time of the authentication token at the second web server.

28. (original) The system of claim 27 wherein the authentication token comprises a cookie.

29. (original) The system of claim 28 wherein the means for transmitting the encrypted authentication token from the first web server to the second web server

comprises means for transmitting the encrypted authentication token from the first web server to the user, and then from the user to the second web server.

30. (original) The system of claim 29 wherein the means for authenticating the user at the first web server comprises means for receiving a user name and password.

31. (original) The system of claim 30 wherein the means for transmitting the encrypted authentication token from the first web server to a second web server comprises means for transmitting the authentication token from the first web server to a computer of the user and means for transmitting the authentication token from the computer of the user to the second web server.

32. (original) The system of claim 31 wherein the first web server and the second web server comprise a federation of web servers.

33. (original) The system of claim 32 wherein the means for authenticating the authentication token at the second web server comprises means for examining the cookie.

34. (original) The system of claim 33 further comprising a means for URL encoding the authentication token.

35. (original) The system of claim 34 further comprising a means for URL decoding the authentication token at the second web server.

36. (original) The system of claim 35 further comprising a means for providing a web page to the user having a service selector.

37. (original) The system of claim 36 wherein the service selector comprises a hyperlink.

38. (original) The system of claim 37 wherein the hyperlink comprises a URL for the second web server.

39. (previously presented) The system of claim 25, further comprising:

a means for sending the digitally signed authentication token to the web browser of the computing device by the first web server; and

a means for sending the authentication token to the second web server by the web browser.

40. (original) The system of claim 39 further comprising a means for allowing the user to conduct a session with the first web server.

41. (original) The system of claim 40 wherein the second web server shares a sub-domain with the first web server.

42. (previously presented) The system of claim 41 further comprising means for digitally signing the authentication token using public key encryption.

43. (original) The system of claim 42 further comprising a means for confirming a match with the digital signature.

44-48. (canceled)